DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

OFFICE OF INFORMATION SERVICES

CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

CIO DIRECTIVE 12-04

DATE: OCT 5 2012

TO: CMS Centers and Office Directors
Consortia Administrators

FROM: Tony Trenkle /s/ CMS Chief Information Officer (CIO) and
Director, Office of Information Services (OIS)

SUBJECT: CIO Directive 12-04 – Revocation/Re-Affirmation of Legacy CIO Directives—INFORMATION

Background

CMS Chief Information Officer (CIO) Directives are used to issue CIO direction on policy-level issues where current direction does not exist. CIO Directives allow the CIO to respond to identified gaps in CMS policy and instruction.

When identified in a CIO Directives, these issues are then integrated into long-term CMS documentation (policies, procedures, security standards, etc.), and the applicable CIO Directive is retired.

Purpose

The purpose of this document is to retire several legacy CIO Directives that have been integrated into CMS policy or other relevant documentation. Other CIO Directives that are being retained are *re-affirmed* as still active.

Implementation

The *status* of each existing CIO Directive, *as of the date of this CIO Directive* (CIO Directive 12-04), are stated below:

1) CIO Directive 07-01—*Transporting Sensitive Information: Encryption Requirements for Data Leaving CMS Data Centers*

   a) **CIO Directive 07-01 is hereby REVOKED.** *Media Transport* requirements are now fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control MP-5: *Media Transport*, and other relevant security controls and enhancements within the ARS.

2) CIO Directive 07-02—*CMS Chief information Security Officer (CISO) Forum for Information System Security Officers (ISSO)*

   a) **CIO Directive 07-02 is hereby REVOKED.** While the *CMS Chief Information Security Officer (CISO) Forum* will continue to occur, the training requirements for *Information*

System Security Officers (ISSOs) are now fully-addressed in CIO Directive 12-03, *Annual Role-Based Information Security Training Requirements* below.

3) CIO Directive 07-03—*Mandatory Encryption on all Removable Storage Devices*

   a) **CIO Directive 07-03 is hereby REVOKED.**
      i) *Whole-disk encryption* requirements are fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control AC-19: *Access Control for Mobile Devices.*
      ii) Additional *data encryption* and *media access* requirements are addressed in other relevant security controls (and their *Enhancements*) within the ARS (including but not limited to: AC-3, AC-17, AC-18, AC-19, MP-4, MP-5, SC-4, SC-7, SC-19, and SC-CMS-1.
      iii) *PointSec™* is currently being phased-out at CMS to be replaced by other FIPS 140-2 compliant solutions. Usage of encryption and access to external storage devices will be governed through network-level *Group Policies,* and set through appropriate CMS Office of Information Services (OIS) management and security standards.
      iv) Use of *personally-owned* equipment is fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control AC-20: *Use of External Information Systems*, and other relevant security controls and enhancements within the ARS.

4) CIO Directive 07-04—*CMS Information Security Incident Handling and Breach Analysis/ Notification Procedure*

   a) **CIO Directive 07-04 is hereby *RETAINED*.** Please continue to follow the instructions contained therein. However, further guidance will be forthcoming on changes to the CMS Incident Response process and associated Privacy Breach reporting processes.

5) CIO Directive 07-05—*FY 2008 Annual Security Controls Testing*

   a) **CIO Directive 07-05 is hereby REVOKED.**
      i) *Annual Controls Testing* requirements are fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control CA-2: *Security Assessments.*
      ii) *Reporting* of annual testing requirements are now fully-addressed in the *CMS Risk Management Handbook (RMH)*, Volume II, Procedure 7.3, *CMS Annual Attestation Procedure.* Additional guidance, and associated changes to this process, will be managed by the CMS CISO, through further issuances and updates to the RMH.

6) CIO Directive 07-06—*Software for Encryption of Agency Information -- Portable Media and E-mail Attachments*

   a) **CIO Directive 07-06 is hereby REVOKED.**
      i) *Electronic Mail* requirements are addressed are fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control SC-CMS-1: *Electronic Mail.*
      ii) Legal requirements for the handling of *Privacy Information* can be found on the CMS *Privacy* website at: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html or by emailing the *CMS Privacy Office* at mailto:Privacy@cms.hhs.gov.

iii) *Data encryption* and *media access* requirements are addressed in other relevant security controls (and their *Enhancements*) within the ARS (including but not limited to: AC-3, AC-17, AC-18, AC-19, MP-4, MP-5, SC-4, SC-7, SC-19, and SC-CMS-1.

iv) *PointSec*™ is currently being phased-out at CMS to be replaced by other FIPS 140-2 compliant solutions. Usage of encryption and access to external storage devices will be governed through network-level *Group Policies*, and set through appropriate CMS Office of Information Services (OIS) management and security standards.

7) CIO Directive 08-01—*Annual Role-Based Information Security (IS) Training Requirements*

   a) **CIO Directive 08-01 is hereby REVOKED.** This Directive has been updated and *superseded* by CIO Directive 12-03— *Annual Role-Based Information Security Training Requirements*

8) CIO Directive 08-02—*Utilization of Webinar Technology at CMS*

   a) **CIO Directive 08-02 is *RETAINED*.** Please continue to follow the instructions contained therein.

9) CIO Directive 09-01—*Use of Personally Owned Equipment with CMS Laptops*

   a) **CIO Directive 09-01 is *RETAINED*.** Please continue to follow the instructions contained therein.

10) CIO Directive 11-01—*CMS Continuous Monitoring Program Implementation*

   a) **CIO Directive 11-01 is *RETAINED*.** Please continue to follow the instructions contained therein.

11) CIO Directive 12-01—*CMS Vulnerability Assessment and Penetration Testing*

   a) **CIO Directive 12-01 is *RETAINED*.** Please continue to follow the instructions contained therein.

12) CIO Directive 12-02—*Minimum Security Configuration Standards*

   a) **CIO Directive 12-02 is hereby REVOKED.** This Directive has been updated and *superseded* by CMS CISO Memorandum—*Minimum Security Configuration Standards,* dated May 3, 2012. Additional guidance, and associated changes to this process, will be managed by the CMS CISO, through further issuances and updates to the ARS and the RMH.

13) CIO Directive 12-03—*Annual Role-Based Information Security Training*

   a) **CIO Directive 12-03 is *RETAINED*.** Please continue to follow the instructions contained therein.

Contacts

If you have questions or require additional information on this Directive, the Enterprise Information Security Group (EISG) team is available to support staff level questions at CISO@cms.hhs.gov.

Tony Trenkle
CIO and Director OIS

cc:
Distribution